Scalable Intrusion Detection for the Emerging Network Infrastruc...

Target Environment

🟥 JiNao Intrusion Detection System

🟩 R IP router 🟦 S ATM switch H Host
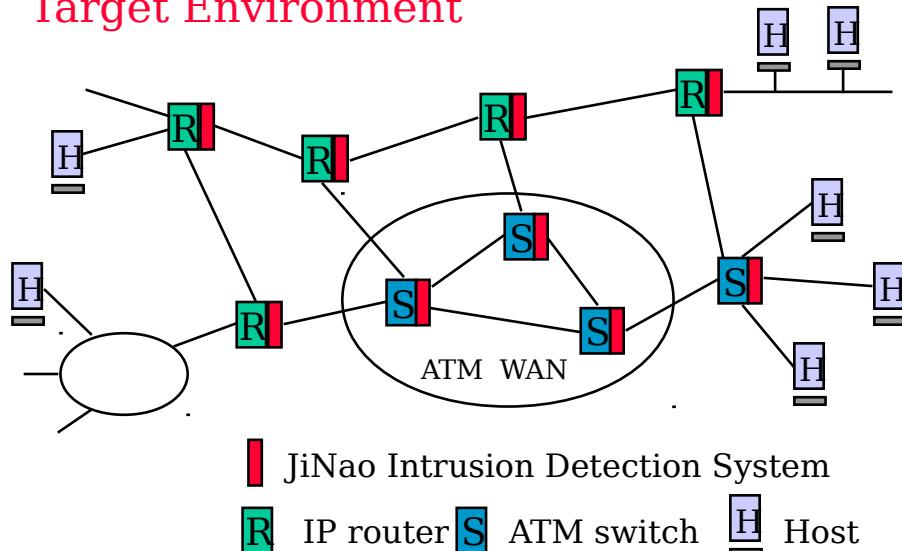
New Ideas

- **Complementary approaches for intrusion detect... infrastructure**
  - Offering prevention, detection, response, and recon... capabilities and able to detect both known and unk...

- **Flexible architecture design which can target at... protocol of interest (currently use OSPF as impl... example), allow dynamic loading/removal of rule... reconfigure system parameters dynamically**

- **Coupling with network management to enable a... responses and easy integration with other system...**

Impact

- **Providing comprehensive capabilities to protect network infrastructures**

- **Resulting better understanding in security implications of key network protocols**
  - Contributing to the IETF and vendors community regarding the the finding of security vulnerabilities in protocol specification and implementation

- **Easy integration to be part of a fault management system through the built-in network management component**

- **Able to serve as a secure wrapper for providing correct implementation to protect the associated nodes**

Schedule

JiNao IDS architecture specification complete

Modules code delivery

Demo of JiNa... implementati... after refinem...

Sep 96
Start

Sep 97

Sep 98 Evaluation Sep 99

Statistical profile delivery

Demo of JiNao system implementation

Final repor...